Chapter 2
Concluded matters

2.1 The committee comments on the following legislative instrument.

2.2 Correspondence relating to these matters is available on the committee's website.[1]

Bills

Intelligence Services Legislation Amendment Bill 2023[2]

Purpose	This bill seeks to amend the *Intelligence Services Act 2001*, *Inspector-General of Intelligence and Security Act 1986* and other legislation for a number of purposes. Schedule 1 would expand the oversight jurisdictions of the Inspector-General of Intelligence and Security and the Parliamentary Joint Committee on Intelligence and Security to include: the Australian Criminal Intelligence Commission, Australian Federal Police, Australian Transaction Reports and Analysis Centre, and Home Affairs. Schedule 2 would make a series of amendments consequential to this proposed expanded oversight jurisdiction. Schedule 3 would designate Australian Criminal Intelligence Commission records relating to a criminal intelligence assessment as exempt security records for the purposes of the *Administrative Appeals Tribunal Act 1975*. Schedule 4 would amend the *Criminal Code Act 1995* to introduce an exemption from certain civil and criminal liability for defence officials. Schedule 5 would make several application and transitional amendments.
Portfolio	Attorney-General
Introduced	House of Representatives, 22 June 2023
Rights	Privacy, effective remedy

1 See https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Scrutiny_reports

2 This entry can be cited as: Parliamentary Joint Committee on Human Rights, Intelligence Services Legislation Amendment Bill 2023, *Report 10 of 2023*; [2023] AUPJCHR 101.

2.3 The committee requested a response from the Attorney-General in relation to the bill in *Report 8 of 2023*.[3]

Exemption from civil and criminal liability for defence officials and others

2.4 This bill seeks to amend 21 Acts to make a range of amendments, many of which relate to expanding the oversight powers of the Inspector-General of Intelligence and Security and the Parliamentary Joint Committee on Intelligence and Security. The committee makes no comment on these broader measures but focuses on Schedule 4. Schedule 4 seeks to amend the *Criminal Code Act 1995* (Criminal Code) to exempt defence officials from civil and criminal liability for certain 'computer related conduct'.[4]

2.5 Computer related conduct would be defined to mean a range of acts, events, circumstances or results involving the use of computers.[5]

2.6 Proposed subsection 476.7(1) provides that a defence official would not be liable for engaging in conduct inside or outside Australia where there was a reasonable belief that it is likely to cause a computer-related act, event, circumstance or result to take place outside Australia (whether or not it in fact takes place outside Australia). Proposed subsection 476.7(6) states that if this conduct causes material damage, interference or obstruction to a computer in Australia, and would otherwise constitute an offence against Part 10.7 of the Criminal Code, the person must provide written notice of the fact to the Australian Defence Force (ADF) as soon as practicable. The explanatory materials state that this proposed measure would ensure that the ADF can use offensive and defensive cyber capabilities for activities connected with the defence and security of Australia, as required as part of modern warfare.[6] As to the type of conduct that may constitute computer-related conduct in this context, the explanatory memorandum states that this may include 'routine activities such as computer intelligence gathering and exploitation'.[7]

2.7 'Defence official' refers to a wide range of persons, and would include a member of the ADF, a defence civilian, an employee of the Department of Defence, a

---

3 Parliamentary Joint Committee on Human Rights, *Report 8 of 2023* (2 August 2023) pp. 64-68.

4 Schedule 4, item 4, proposed section 476.7.

5 Schedule 4, item 1, proposed amendment to subsection 476.1(1) would insert a definition of 'computer related conduct'. Computer related conduct means an act, event, circumstance or result involving: the reliability, security or operation of a computer; access to, or modification of, data held in a computer or on a data storage device; electronic communication to or from a computer; the reliability, security or operation of any data held in or on a computer, computer disk, credit card, or other data storage device; possession or control of data held in a computer or on a data storage device; or producing, supplying or obtaining data held in a computer or on a data storage device.

6 Statement of compatibility, p. 14, and explanatory memorandum, pp. 159–160.

7 Explanatory memorandum, p. 159.

consultant or contractor to the department, or any other person specified in a class of persons by the secretary or Chief of the ADF by legislative instrument.[8]

2.8 Proposed subsection 476.7(2) would further provide an exemption from civil or criminal liability for people who engage in activities, inside or outside Australia, that are preparatory to, in support of, or otherwise directly connected to overseas computer- related activities.[9]

Summary of initial assessment

Preliminary international human rights legal advice

Rights to privacy and an effective remedy

2.9 Exempting persons from civil or criminal liability for computer related conduct engages and may limit the right to an effective remedy, should that conduct result in a breach of the civil and political rights of a person in Australia (such as the right to privacy).

2.10 The statement of compatibility states that these amendments may 'indirectly create a risk that' a person's right to privacy may be violated, including where conduct has inadvertently affected a computer or device inside Australia.[10] This suggests that the exercise (or purported exercise) of this power may result in a limitation of the right to privacy in Australia.[11] It is therefore necessary to consider whether such a limitation on the right to privacy would be permissible should this take place, and whether an affected person would have access to an effective remedy.

Committee's initial view

2.11 The committee noted that exempting persons from civil or criminal liability for computer related conduct engages and may limit the right to privacy of a person in Australia, and consequently may also engage the right to an effective remedy. The committee sought the Attorney-General's advice as to:

---

8 Schedule 4, item 4, proposed subsection 476.7(8).

9 Schedule 4, item 4, proposed subsection 476.7(3) states that this is not intended to permit any conduct in relation to premises, persons, computers, things, or carriage services in Australia being conduct which the Australian Security Intelligence Organisation (ASIO) could not engage with or obtain under specified legislation.

10 Statement of compatibility, p. 14.

11 In this regard, it is noted that Schedule 4, item 4, proposed subsection 476.7(2) would exempt 'a person' from liability for conduct preparatory to computer-related conduct (whereas proposed subsection 476.7(1) would exempt a defence official), and so would appear to potentially exempt a far broader range of persons from liability. It may also be that, in practice, computer-related conduct may directly or indirectly limit other rights, as a consequence of a particular breach of the right to privacy, depending on the nature of the conduct and the context.

(a) whether, where the exercise of this power limits a person in Australia's right to privacy, this would constitute a permissible limitation on the right to privacy, and whether any other human rights may be limited in such circumstances;

(b) whether the measure is consistent with the right to an effective remedy; and

(c) what alternative remedies are available to persons where conduct contemplated by proposed section 476.7 results in a violation of their human rights.

2.12 The full initial analysis is set out in *Report 8 of 2023*.

Attorney-General's response[12]

2.13 The Attorney-General advised:

> **Engagement with the right to privacy**
>
> The Bill provides 'defence officials' with immunity from criminal and civil liability for computer-related activities done in the proper performance of approved Australian Defence Force (ADF) activities and on the reasonable belief that they will take effect outside Australia. While the Bill does not have the effect of directly limiting the right to privacy, the Bill indirectly creates a risk that a person in Australia's right to protection against arbitrary and unlawful interferences with privacy under Article 17 of the ICCPR may be violated.
>
> **Permissible limitation of the right to privacy**
>
> The amendment pursues the legitimate objective of protecting defence officials from personal liability when utilising cyber capabilities for activities connected to the defence and security of Australia. Limitation of the right to privacy is necessary to ensure that the ADF can counter serious threats to Australia's national security. Protecting defence officials from liability for engaging in such conduct, in the proper performance of ADF activities, is necessary to ensure those officials can undertake necessary cyber activities without fear of personal liability.
>
> The immunity is proportionate, as it is limited to circumstances where defence officials engage in conduct in the proper performance of authorised ADF activities, including in compliance with rules of engagement and other applicable processes and procedures. Defence officials will not be immune for conduct engaged in otherwise than in the proper performance of an authorised ADF activity.

---

12 The minister's response to the committee's inquiries was received on 1 September 2023. This is an extract of the response. The response is available in full on the committee's webpage.

It is not always possible for a defence official to be certain as to the location of a computer or device online, particularly where an adversary takes active steps to conceal or obfuscate their location. Protecting defence officials from liability in such circumstances is necessary to ensure that those officials can undertake such activities on the reasonable belief that their conduct will take effect outside Australia, without fear of personal liability if their belief turns out to be mistaken. A defence official will not be immune if they believe that their conduct will take effect inside Australia nor if their belief is not reasonable in the circumstances.

The amendment also requires that a person must provide written notification if they engage in conduct that causes material damage, material interference or material obstruction to a computer in Australia. This notification will go to the Chief of the Defence Force (CDF) for persons who fall under the CDF's command and to the Secretary of the Defence Department in other cases. The notification process will facilitate consideration at the most senior levels within Defence of any necessary or appropriate internal review processes, to ensure accountability. Such review could include consideration of the legal basis for the original conduct, or operational review to ensure computer capabilities were used appropriately and in line with Defence standard operating procedures. The CDF and Secretary of Defence would also be able to take steps to remedy any issues identified in such an internal review, such as updating procedures and guidelines, and take any disciplinary action.

Right to an effective remedy and alternative remedies

Article 2(3) of the ICCPR protects the right to an effective remedy for any violation of rights or freedoms recognised by the ICCPR, including the right to have such a remedy determined by the competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State. The right to an effective remedy applies notwithstanding that a violation has been committed by persons acting in an official capacity. Accordingly, the Bill engages the right to an effective remedy for any unlawful or arbitrary violation to the right to privacy.

While a person who has been adversely affected by this conduct would not be able to take civil action against the defence official involved, a person may still be entitled to claim compensation or remedial relief from the Commonwealth. For example, and depending on the particular circumstances, a person may be able to seek and obtain compensation or remedial relief for alleged defective actions under the Compensation for Detriment caused by Defective Administration or an act of grace payment under the *Public Governance, Performance and Accountability Act 2013*. Complaints may also be able to be made to the Office of the Australian Information Commissioner or the Defence Ombudsman.

Concluding comments

International human rights legal advice

2.14 The Attorney-General advised that the bill does not directly limit the right to privacy but does indirectly create a risk that the right to privacy of a person in Australia may be violated. As to whether this would constitute a permissible limitation on the right to privacy, the Attorney-General stated that the amendment seeks to protect defence officials from personal liability when they are utilising cyber capabilities for activities connected to the defence and security of Australia. They further advised that the immunity is limited to circumstances where defence officials engage in conduct in the proper performance of authorised ADF activities, including in compliance with rules of engagement and other applicable processes and procedures.

2.15 However, it remains unclear whether, and to what extent, 'computer-related conduct' as captured by the proposed immunity may limit the right to privacy of persons in Australia. As this bill does not itself appear to empower defence officials to undertake such activity, it is unnecessary to conclude whether any such limit on the right to privacy is permissible. However, if such conduct did impermissibly limit the right to privacy (or limit any other civil and political right) of a person in Australia, that would engage the right to an effective remedy.

2.16 In relation to the right to an effective remedy, the Attorney-General advised that a person who had been adversely affected by this conduct may be entitled to claim compensation or remedial relief from the Commonwealth, such as through the Compensation for Detriment caused by Defective Administration or an act of grace payment under the *Public Governance, Performance and Accountability Act 2013*. The Attorney-General also noted that complaints may also be made to the Office of the Australian Information Commissioner or the Defence Ombudsman.

2.17 If, despite the proposed immunity, a person was able to seek relief from the Commonwealth this may meet the requirements for an effective remedy. However, it is not possible to conclude whether the remedies the Attorney-General has identified would constitute *effective* remedies for the purposes of international human rights law (noting that whether a remedy is effective may depend on the nature of the rights breach in question). Further, it is unclear how an affected person would know that any such detriment was due to conduct for which the Commonwealth was accountable (noting that these activities would appear to be covert). In this regard, the Attorney-General stated that if a person had engaged in conduct that caused material damage, material interference or material obstruction to a computer in Australia, the Chief of the Defence Force would need to be notified in writing. The Attorney-General stated that this notification process would facilitate senior departmental consideration of any necessary internal review processes, which could include consideration of the legal basis for the original conduct, or operational review to ensure computer capabilities were used appropriately and in line with Defence standard operating procedures. However, these steps would appear to provide internal oversight and review but

would not appear to include notifying the person who suffered the detriment of the conduct or provide a remedy to that person.

Committee view

2.18 The committee thanks the Attorney-General for this response. The committee notes the Attorney-General's advice that these proposed immunities seek to protect defence officials from personal liability when utilising cyber capabilities for activities connected to the defence and security of Australia. The committee further notes the Attorney-General's advice that when defence officials engage in computer-related conduct there is a possibility that this may limit the right to privacy of people in Australia. However, the committee considers that it is not clear to what extent Australians' privacy may be limited. The committee considers that if such conduct did impermissibly limit the right to privacy of a person in Australia, that would in turn engage the right to an effective remedy.

2.19 The committee notes the Attorney-General's advice that a person who suffered detriment as a result of the conduct contemplated by this measure could seek compensation and other relief from the Commonwealth, and considers that some remedies may therefore be available. However, the committee considers that because the extent of any potential inference with the right to privacy is not clear, it is not possible to conclude whether these identified remedies would be considered to be effective remedies for the purposes of international human rights law.

2.20 The committee draws these human rights concerns to the attention of the Attorney-General and the Parliament.

Mr Josh Burns MP

Chair